Using Digipass Strong User Authentication with Novell NMAS and ICHAIN

Using Digipass Strong User Authentication with Novell NMAS and ICHAIN

Contents

Contents 2
Overview 3
Situation – Description 3
Solution 3
Technical Concept 4
Topology 4
Novell Components Description 5
NMAS 5
ICHAIN 5
VASCO Components Description 6
Digipasses 6
Databases and Files 8
Configuration Parameters 9
Configuration of IChain 9
Configuration of NMAS 12
Configuration of Radius 23
Configuration of Web 24
Conclusion 24
Appendix A – Delta Airlines Access Examples 25
Authentication – Authorization over IChain secured 25
Appendix B Local Network Logon 28
VASCO – Challenge Response Authentication 28
Appendix C – The VASCO VRM & Tokens work with BM (BMAS) VPN Services 30
VPN Secure Authentication with The Digipass 300 and the Digipass Go-1 with PIN+RESPONSE 30
About VASCO Data Security 30
General 30
Digipass product range 31
Digipass Pro: 31
Digipass GO: 32
Digipass Desk: 32
VACMAN product range 32

Overview

This document shows you how Novell IChain and NMAS optimizes its authentication by integrating VASCO Digipass for strong user authentication and offering several secure web and RADIUS access solutions.

Situation – Description

As electronic connectivity, where hackers, viruses, electronic eavesdropping and fraud can threaten the communication, productivity and prosperity of business and individuals, advanced network authentication-based solutions are becoming a necessary component in corporate security policies.

Advanced network authentication lessens the threat of intrusion by requiring the users to provide stronger authentication credentials and by allowing for the creation of multi-factor login sequences.

Ideally, advanced authentication methods should be managed in a complementary advanced authentication framework that supports the access of network resources. In addition, the framework should be secure enough so that information accessed through one form of authentication cannot be moved to a network area requiring a different form of authentication.

To be more specific: we need access to our resources stored on the server at the headquarter at any time from anywhere with maximum of security.

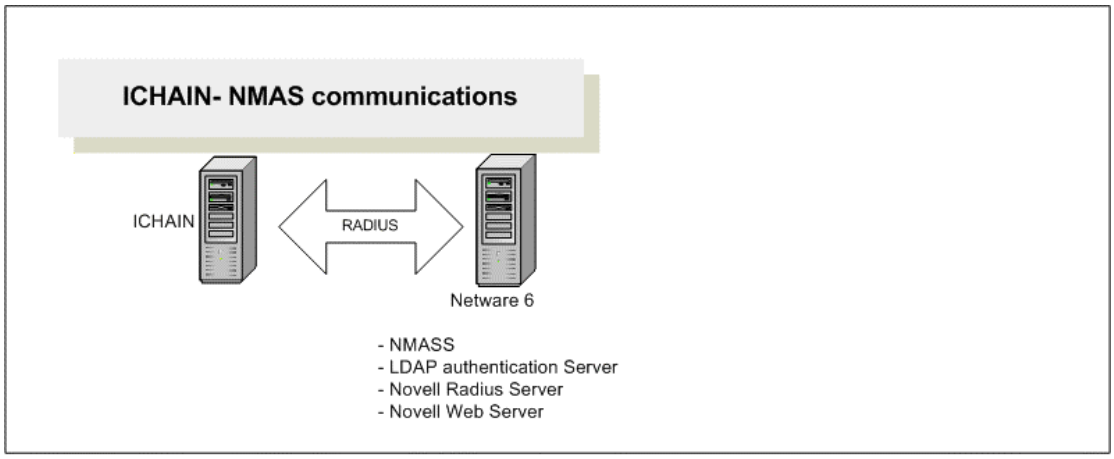
Solution

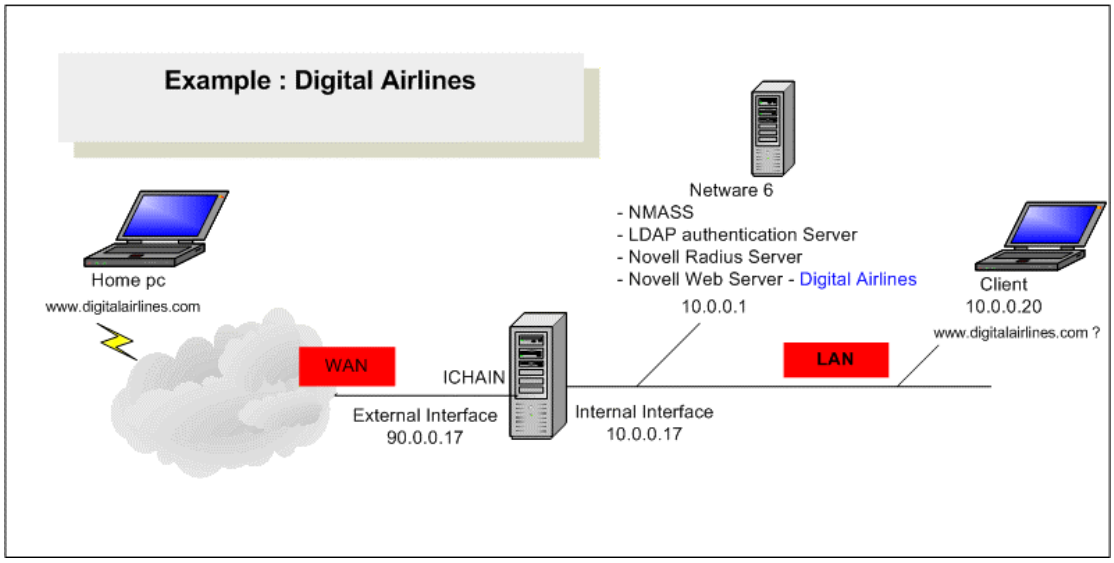
Novell Modular Authentication Service (NMAS) adds value to authentication while IChain offers the flexibility of connecting over several frameworks without requiring a different form of authentication. VASCO Digipass adds value to this structure by requiring a non-static password. Digipass enables users to create a one-time-password (OTP) that safeguard access to e-business and banking applications, to corporate networks. With a combination of information that a user needs to remember and information he gets, like a one time password, you eliminate the weakest link in any security infrastructure. NMAS has a built-in VASCO Digipass Authentication Module which verifies the OTP before granting access to secured resources.

Technical Concept

Topology

Concept – Fig





Novell Components Description

NMAS

Novell® Modular Authentication Service is an extensible security product that offers you an easy way to centrally manage multiple authentication methods across your network. With Novell Modular Authentication Service, you can implement stronger forms of authentication and authorization to secure your critical corporate resources. While removing the complexity of authentication to Novell eDirectory™, Novell Modular Authentication Service allows you to create a variety of flexible security options. Novell Modular Authentication Service also helps remove the administrative overhead involved with maintaining password information throughout your organization.

With Novell Modular Authentication Service, users can authenticate to the network via something they know (for example, a password), something they have (for example, a Digipass), or something they are (for example, a fingerprint).

By supporting the leading smart card, proximity card, token, biometric and digital-certificate vendors authentication products, Novell Modular Authentication Service provides a way to centrally and easily manage your authentication methods. In addition to its administration features, Novell Modular Authentication Service also offers graded authentication. With graded authentication you can create a security policy that grants access to your file system or directory resources based on the strength and combination of the authentication. For example, you can create a method that requires a user to log in with a password, present a valid smart card ID and successfully complete fingerprint identification. By including graded authentication and support for various Novell and third-party authentication modules, Novell Modular Authentication Service provides you with several security options and ensures that your network will not be compromised by a carelessly handled password.

ICHAIN

Novell® IChain® is an identity-based security product that controls access to application, Web and network resources across technical and organizational boundaries. Novell iChain separates security from individual applications and Web servers. This enables single-point, policy-based management of authentication and access privileges throughout the Net. Novell iChain optimizes eBusiness-application development by leveraging fine-grained security that transcends firewalls. As a result, businesses can simplify Net access and security management, based on users' identities. Businesses can also control the use of digital assets across the extended enterprise and get more—faster—from investments in eBusiness applications.

With Novell iChain you can move your business online without sacrificing security. To support your organization's transformation to eBusiness, Novell iChain includes the following enhancements.

- Customizable login pages
- Multi-factor authentication

- Proxy-server clustering
- Server fault tolerance
- Support for Remote Authentication Dial-In User Service protocol (RADIUS)

Novell iChain is the ideal product to secure and accelerate your company's transformation to eBusiness. It is also a key component of Novell Secure Access™, Novell's comprehensive security suite.

VASCO Components Description

Digipasses

Digipass Family of tokens is a general name used by VASCO to describe the family of handheld security devices that VASCO manufactures and markets.

Digipass tokens are security devices that were originally developed as an answer to the use of easy to compromise static passwords and PIN codes because:

- Incorrect authentication is the single largest threat to any computer system

- User-managed passwords are the single largest cause of incorrect authentication

VASCO delivers strong authentication and guarantees data integrity for electronic transactions by means of the Digipass Family of Tokens. In the concept, we implemented the cures for the weak areas of authentication and data integrity. To avoid the static nature of passwords, we needed something that delivered dynamic passwords, was highly portable and flexible to integrate into any environment and on top of that, not expensive. In other words, we needed to implement strong security with a maximum of flexibility and a minimal total cost of ownership. We considered security to be a trade-off between: security, flexibility, price and ease of use and therefore developed the Digipass tokens.

What is a Digipass token?
A Digipass token is a handheld device that calculates dynamic passwords, also known as One Time Passwords (OTP), for the positive authentication of a user on a remote system. It is also able to calculate digital signatures also known as electronic signatures, or Message Authentication Codes (MAC), to protect electronic transactions and guarantee the integrity of the contents of these transactions.

The calculation of these OTP's and MAC's is based upon the publicly available Data Encryption Standard (DES) algorithm. The DES algorithm is proven to be strong in numerous fields of application by renowned institutions and industry leading companies. To provide an even higher level of security the Triple DES algorithm is supported as well.

Security has three factors:
- What you have (the Digipass token itself)
- What you know (the PIN code to activate the Digipass token)
- Who you are (biometrics, voice, retina scan, fingerprint, etc.)

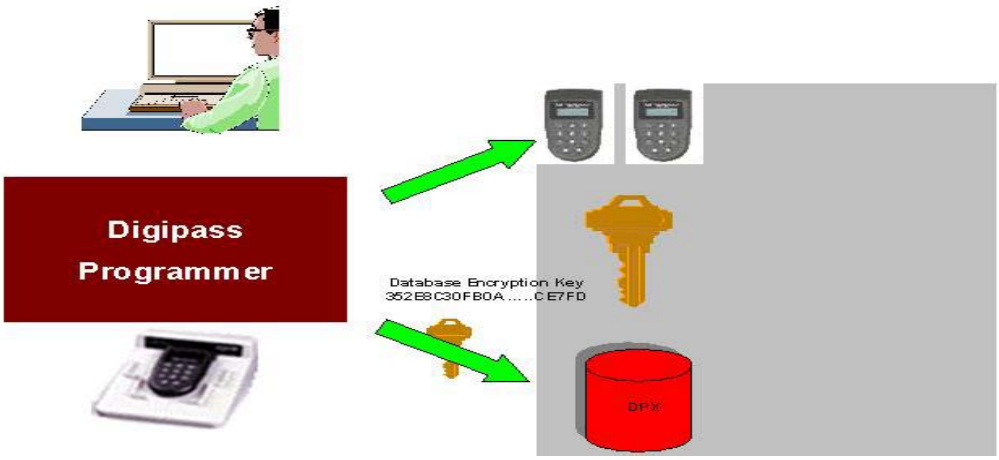
Since the biometrics industry today is still in the development stage and products in this area tend to be extremely expensive, we based the Digipass Family of tokens on the first two factors of the list. This means that in order to enter a remote system or to digitally sign data you need the hardware device itself (factor 1). This means that if you do not physically have the token you will never be able to log on to the system. On top of that you need to know the PIN code for the token (factor 2), to be able to use the applications stored inside. Both of these factors help to make sure that a physical person is authenticating or signing instead of a computer or another device.
These factors also enable extremely high portability. Therefore, we say that you can use a Digipass token Anytime, Anywhere and Anyhow.

Technical Description
In the technical description on our Digipass Family of tokens we will elaborate on the three (3) most frequently used implementation modes of the DES algorithm in conjunction with

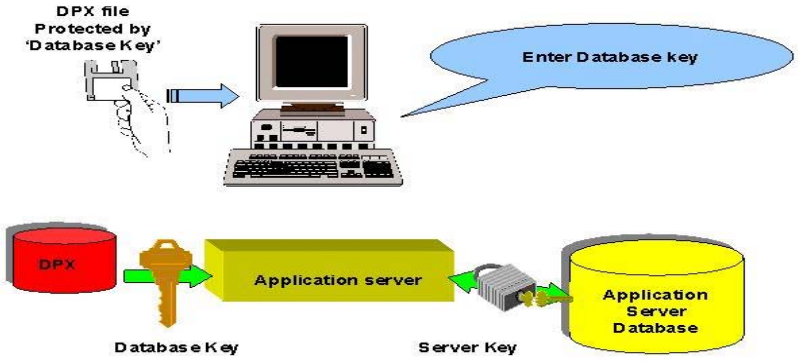
our Digipass Family of tokens. These modes are the Response-Only mode, the Challenge-Response mode and the Digital Signature mode. But first we will start by showing you the complete application cycle of the Digipass token usage.

Databases and Files

General concept for Digipass Family hardware token usage



(Fig 1a) The first step is the tokens are initialized with their unique set of secrets and keys per token. These secrets are stored in an encrypted way on a diskette which is sent to the application owner (e.g. the security department of a bank or the IT manager in a company). These floppies are a way of safely transporting the Digipass secrets to the host computer. The files on the floppy disks will be used to read all the necessary secrets and other data from the Digipasses that were delivered into a database.



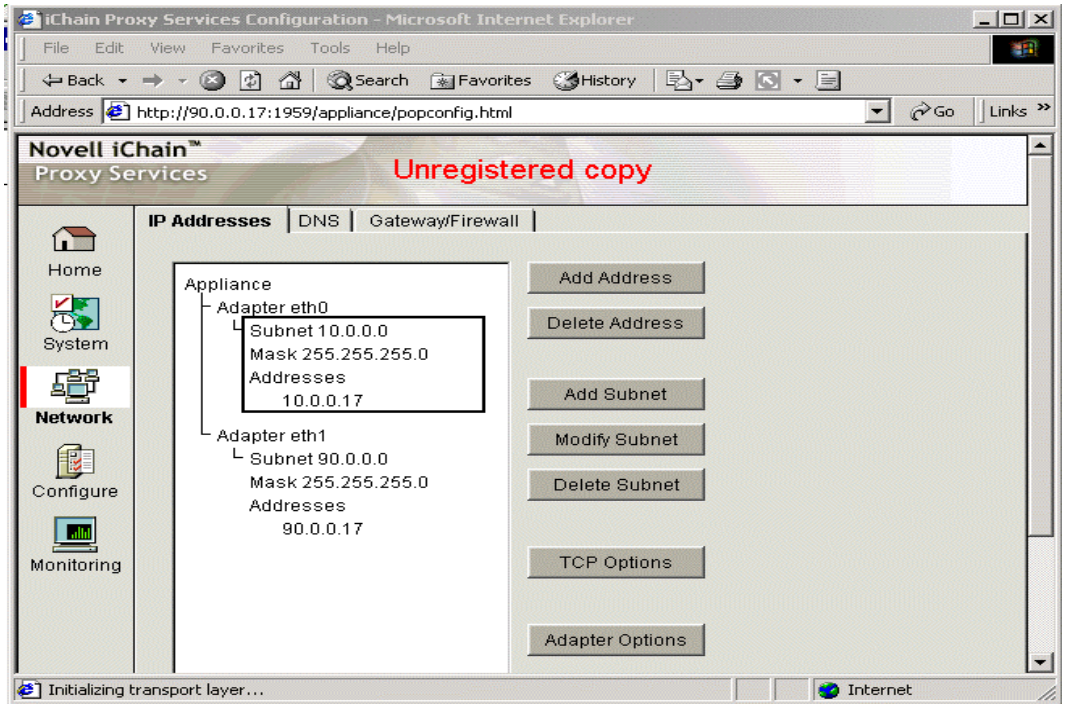
(Fig 1b) Once this is done, the application owner will assign those Digipass secrets to their end-users. This assignment is done based on the serial number of the Digipass token and the name of the end-user. The Digipass token is then shipped to the end-user together with a manual and the protected PIN-code on a secure PIN-mailer.

Once the token is received by the end-user, he can start using it. To use a Digipass you need a connection to the host (server) computer that knows the secrets of the end-user's Digipass token. Every time the user sends a dynamic password or digital signature to the host computer, the computer will get all the necessary information from the database and will check the validity of the password or signature. After the host has checked the validity of the dynamic password or signature, he will notify the end-user of the correctness or incorrectness of the validity check

Configuration Parameters

Configuration of IChain

Fig 2. Configuration of IP address for proxying



As access is needed from an external resource to an internal resource, two subnets are configured in order to handle all requests from outside. As in our example with the Delta

Airlines site (web server 10.0.0.1), two subnets are configured. As the local data or e-business applications resides on the 10.0.0.0 subnet (Fig 3), address translation will enable transparent access.

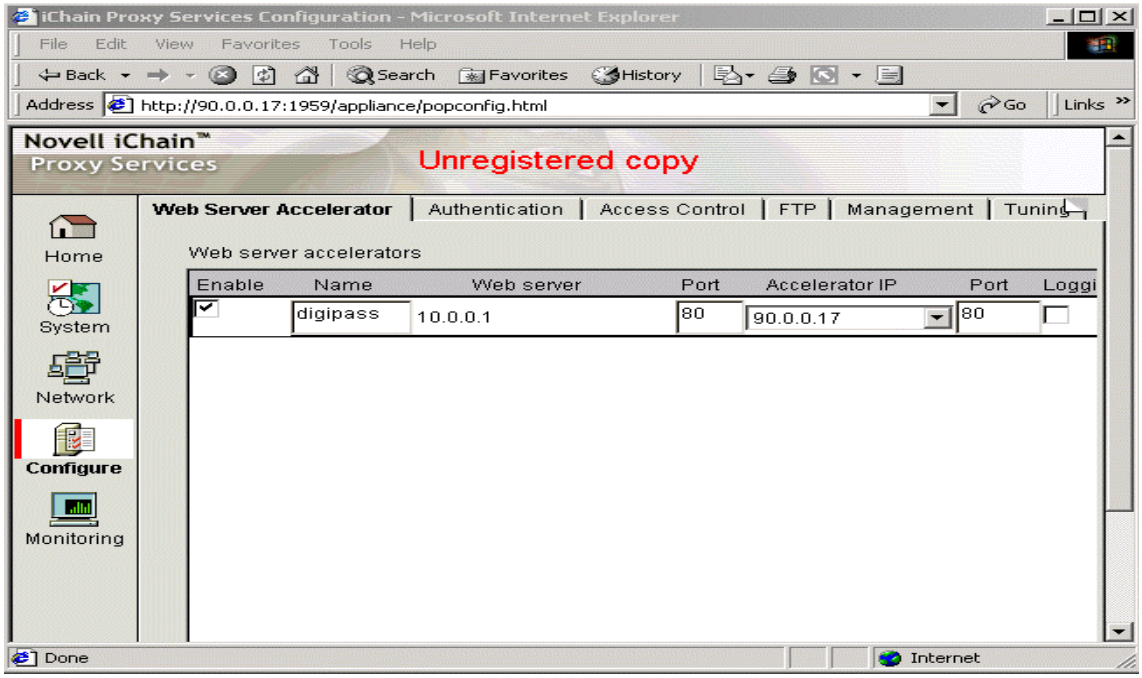


Fig 3

Radius will be the Protocol used for Authentication, as such, a Radius profile needs to be configured. Fig 3a, 3b

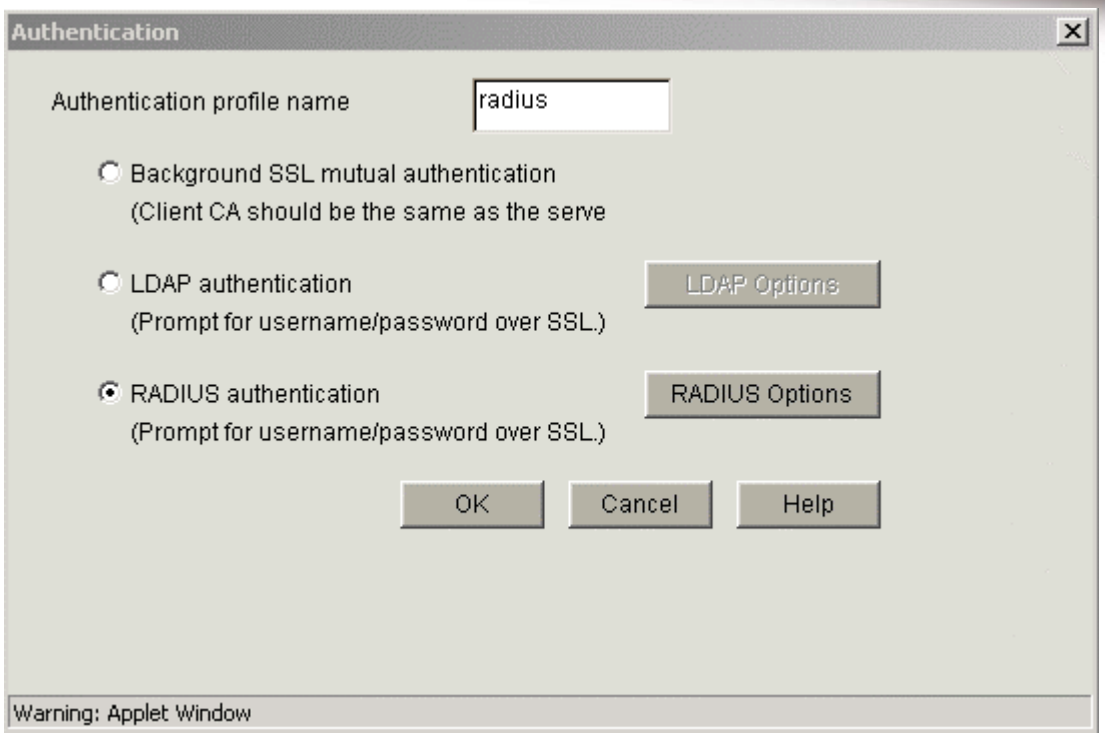


Fig 3a Select authentication, then select radius authentication.

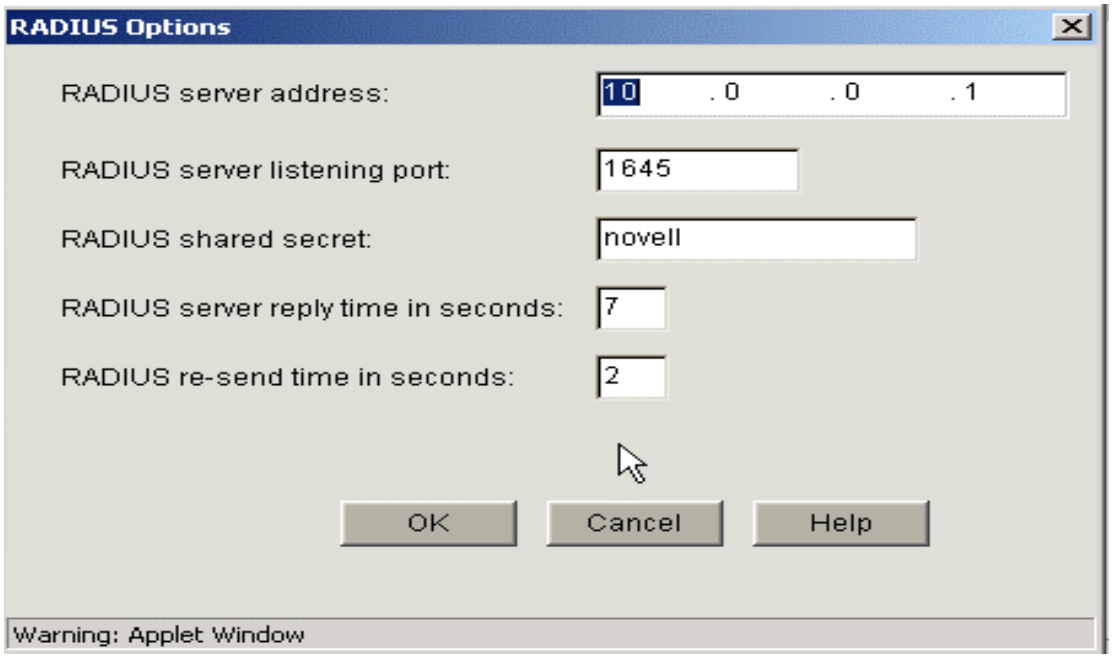


Fig 3b Configure the IP Address of the Radius Server

NMAS System Settings

In this section we need to configure the type of services to be used in order to access its' resources. The services are user-related.
Configuring Radius Access is done in two steps :

1. Add the Radius Dial Access Service
2. Add the Radius Dial Access Protocol (Here we can provide attributes or we can just use the default setting.) In this case default settings are used.

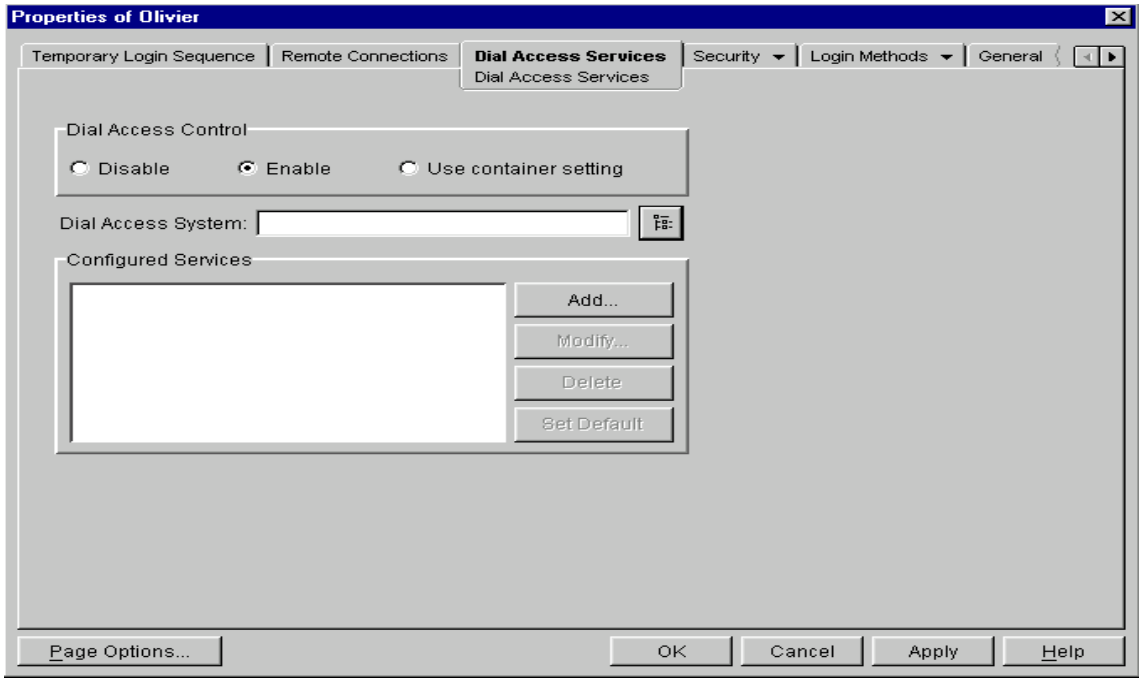
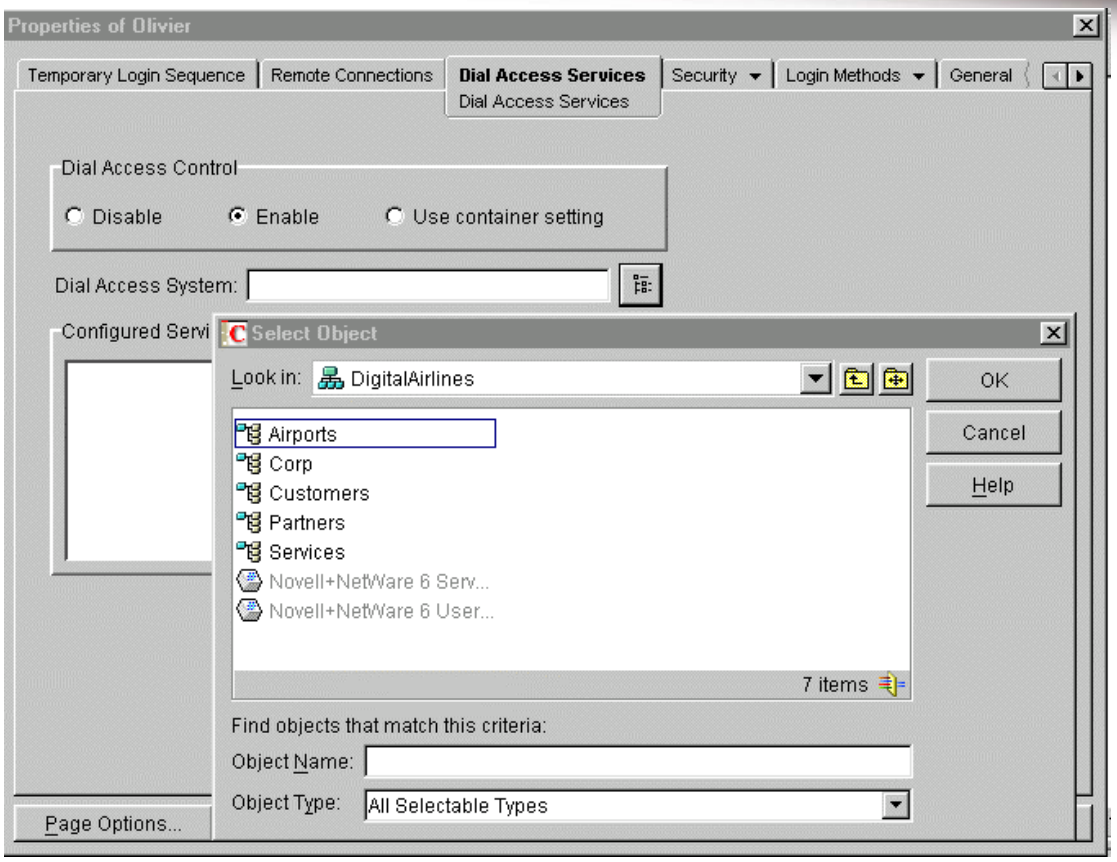
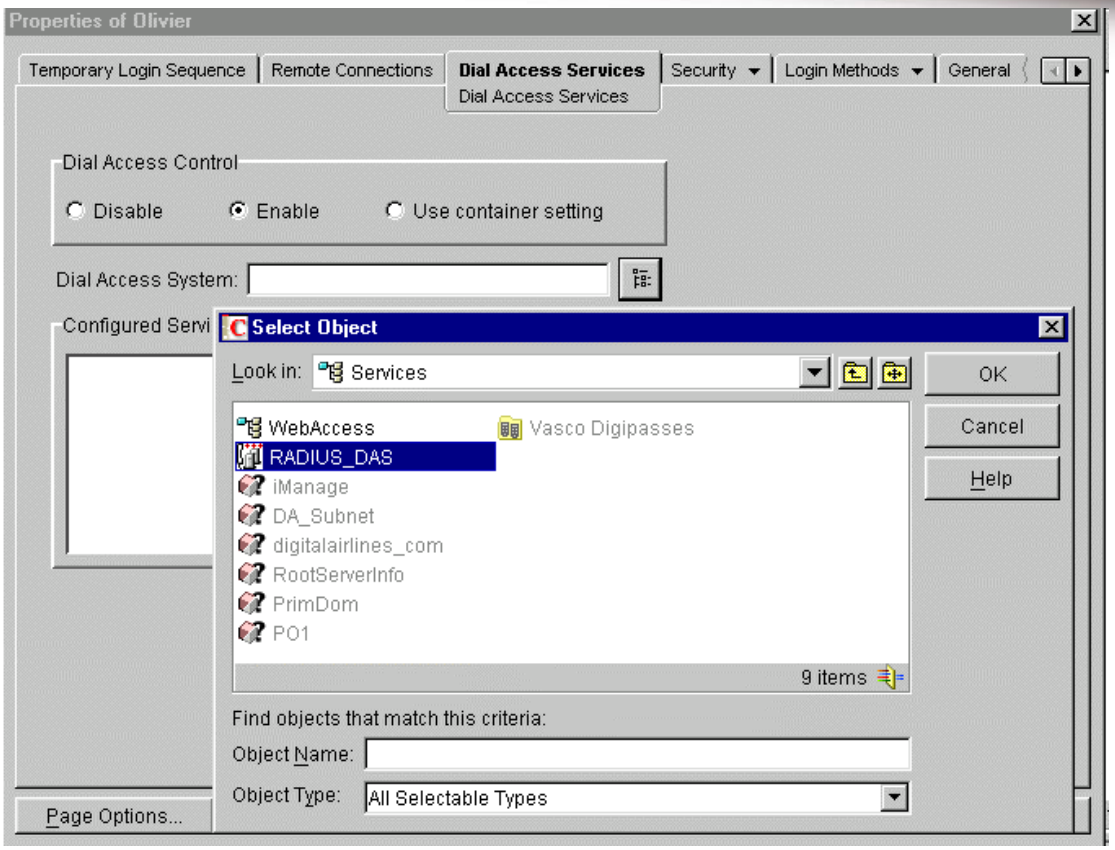


Fig 4a Enable Dial Access Control.

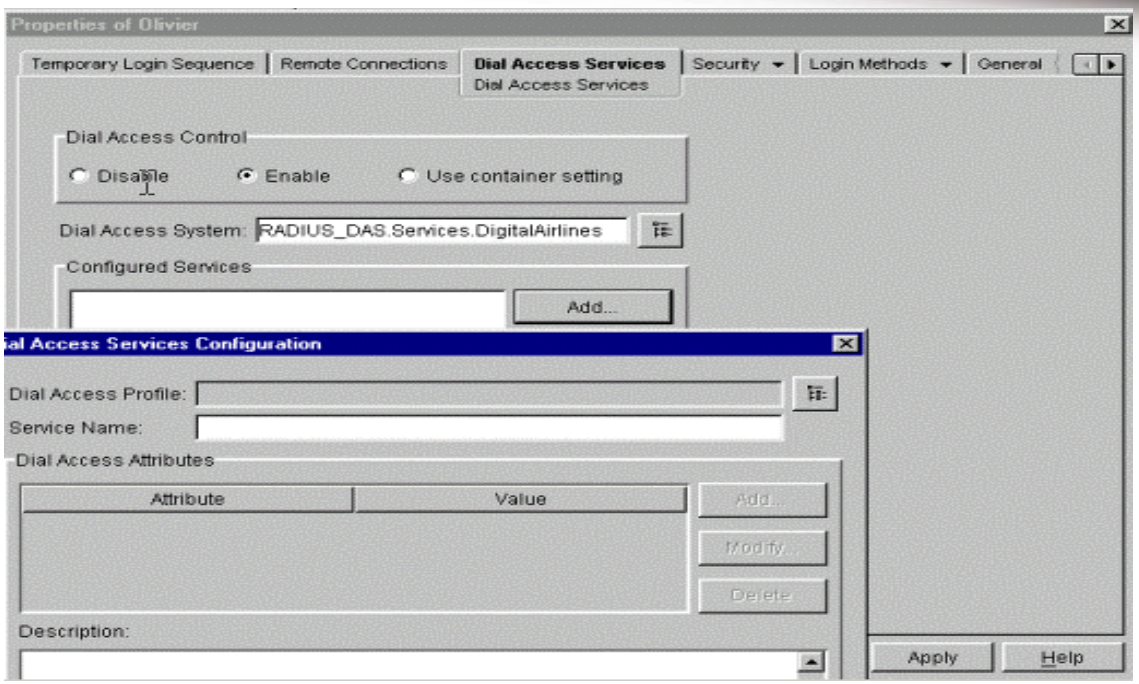
In order to use Radius, we need to specify Radius Dial Access.



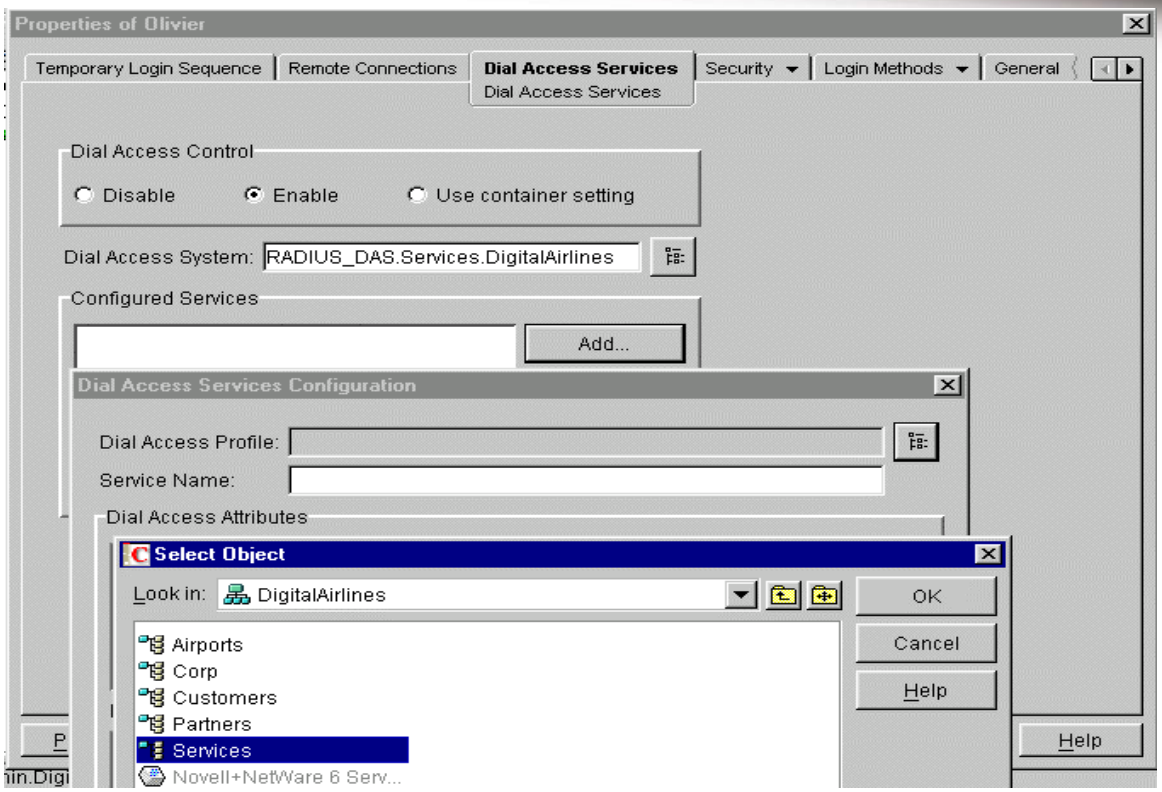
Services represents the Radius Dial Access Protocol. Double click on Services



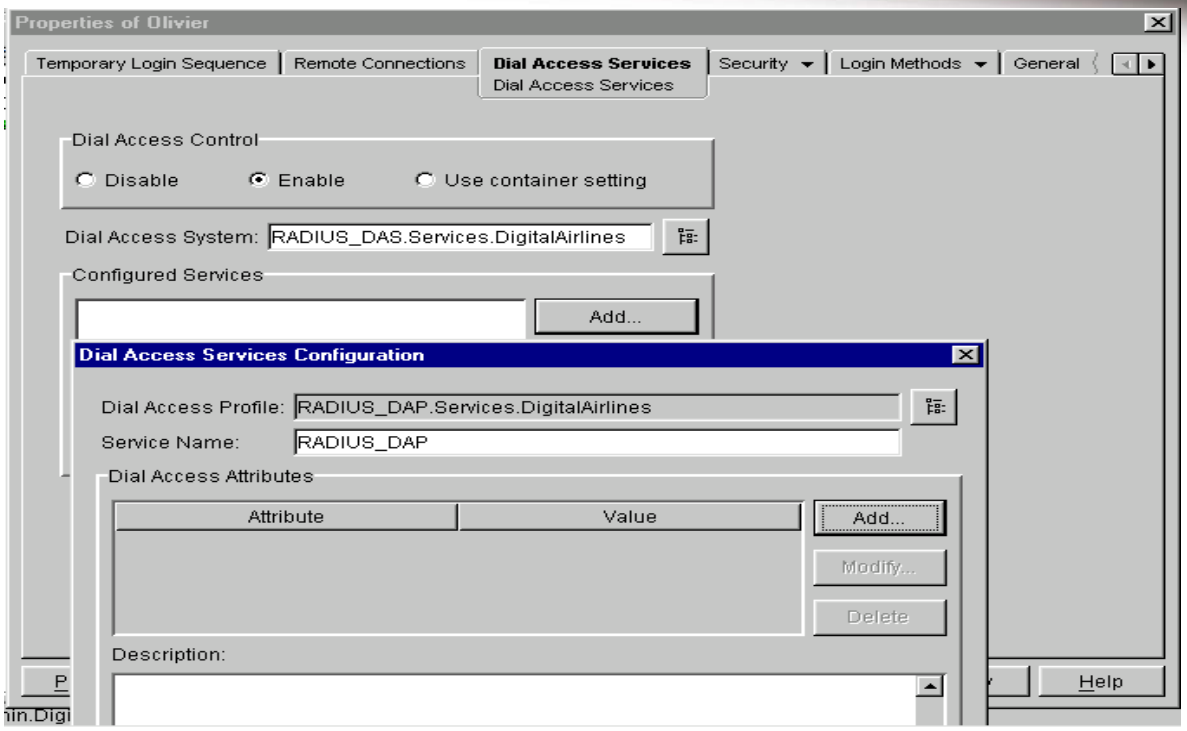
Select the RADIUS_DAS Service.



We finished configuring the Radius_DAS Service. Now we need to specify the Radius Protocol . For example Callback , …..
Click Add to configure.



Once again select Services.



Select RADIUS_DAP and click OK. You can rename it to Radius Dial Access Protocol.
When no method is specified, adds `default` .
Example. Radius Dial Access Protocol. [DEFAULT]

NMAS VASCO Digipass import

Configure VASCO Digipass container

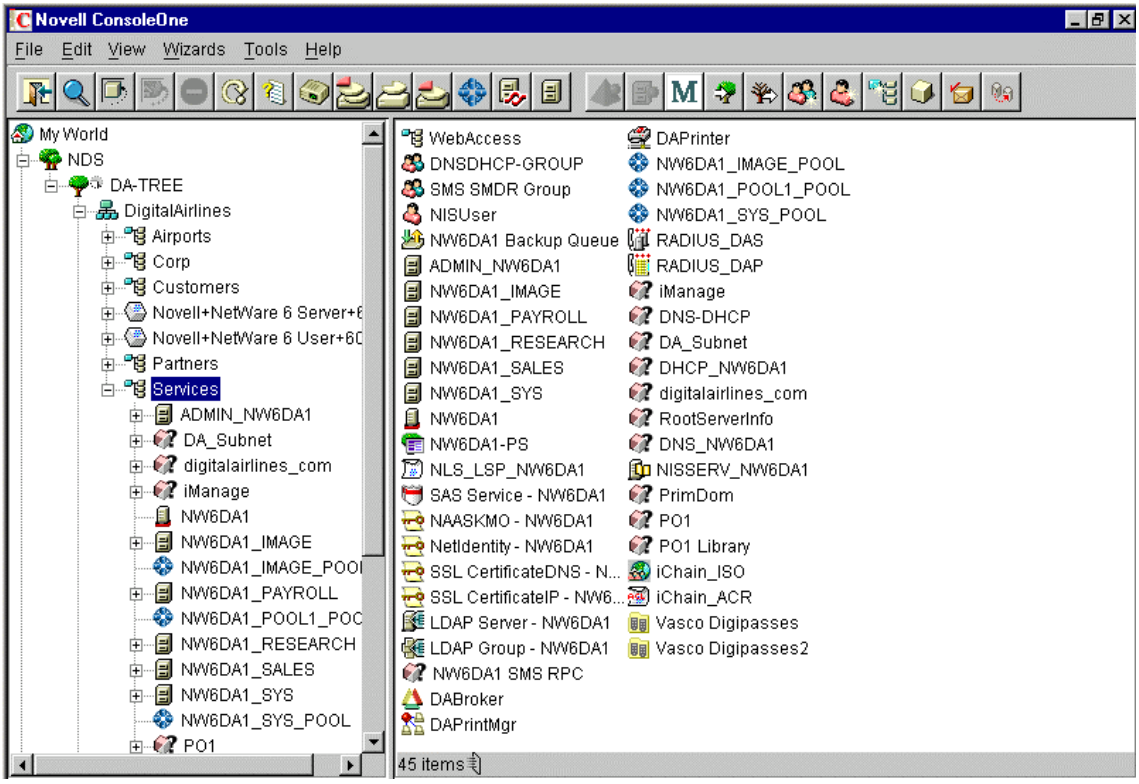


Fig 5

As NMAS has VASCO integrated, there is only the need to configure the service and activate it.Configuration of a container for Digipasses is done through creating a new object in Services. Fig 5

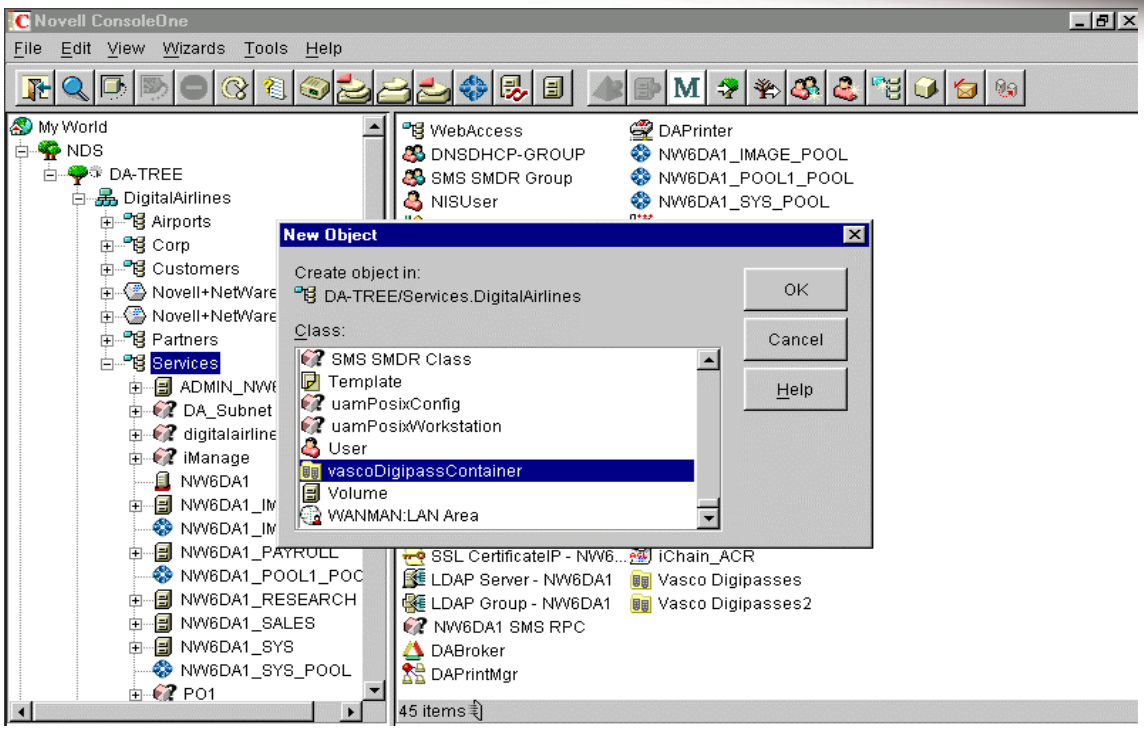


Fig 6

VASCO Digipass container will contain the VASCO Digipass token object, for which you can give a friendly name. Fig 6

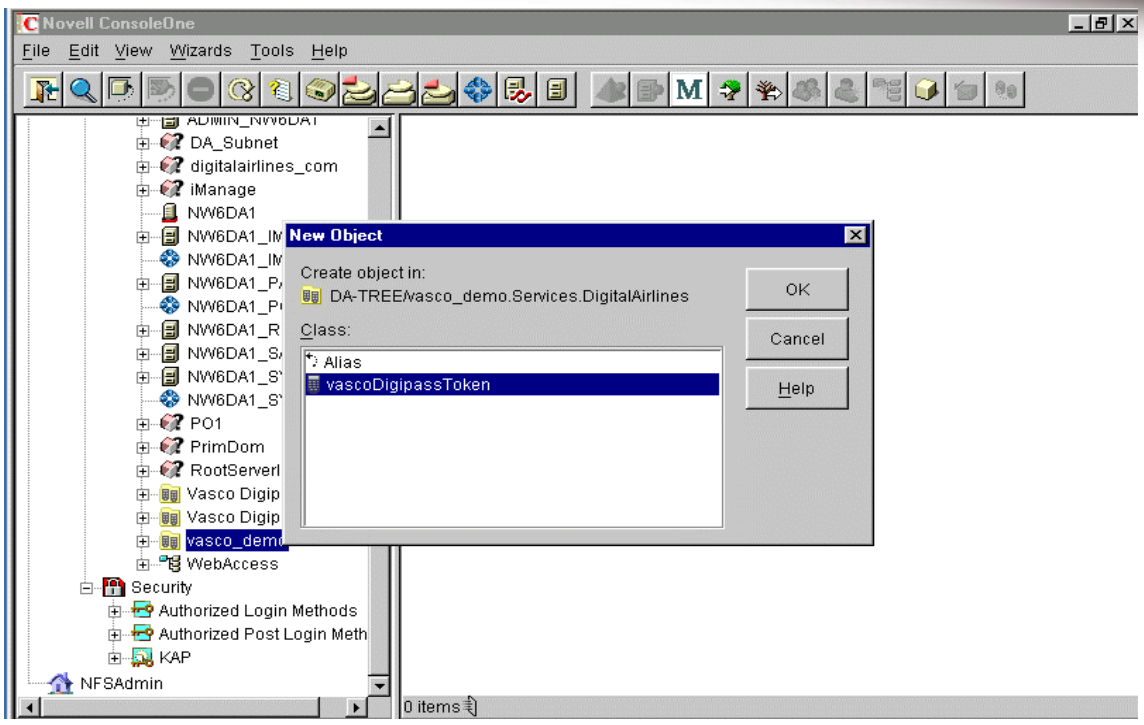


Fig 7

For importing tokens, a VASCO Digipass token object is created. This object will contain all Digipasses and their functions conform the initialization sheet. This is also the location where a user will be assigned a Digipass. Fig 7. In order to import tokens, the location of the dpx file and its' encryption key need to be provided.

Import Dpx files

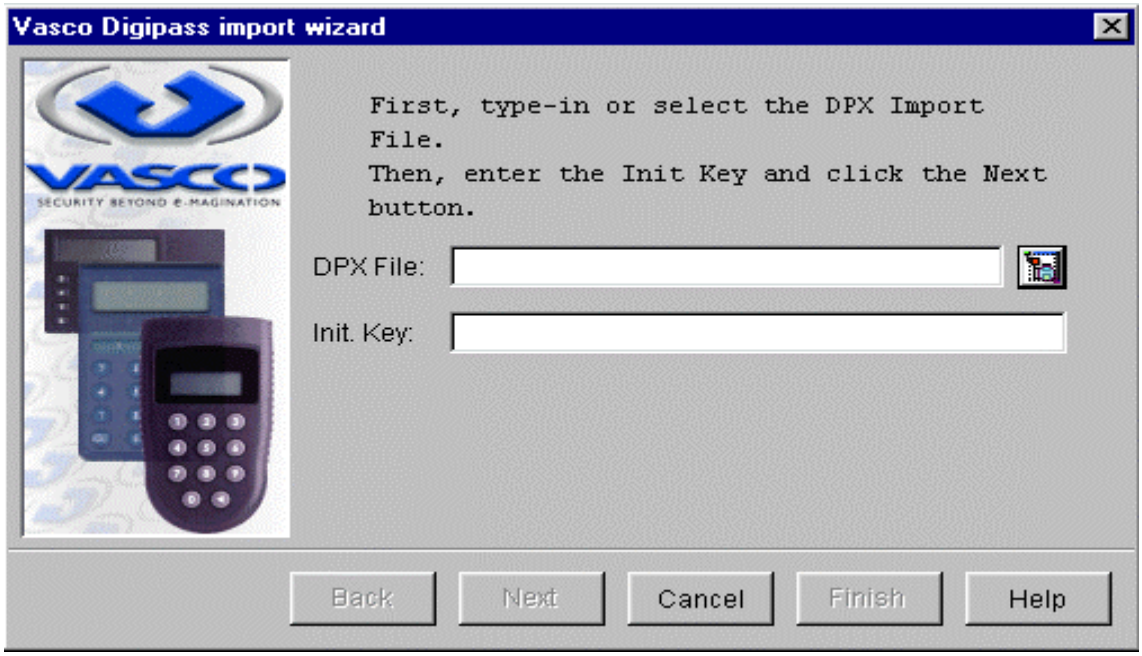


Fig 8.

This is also the location where a user will be assigned a Digipass. Fig 8. In order to import tokens, the location of the dpx file and its' encryption key need to be provided.

NMAS User-VASCO Digipass Management

Assignment users

In this section we need to configure type of authentication a user is configured for and the type of services it will use in order to access its' resources.

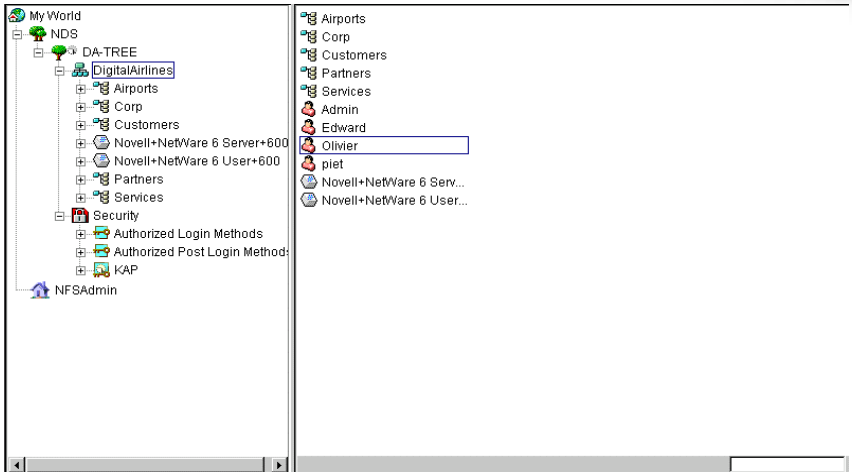


Fig 9

Fig 9 represents the DNS structure where Digital Airlines is the applicationas well as the container where all users accessing it, will be registered and given permissions, levels of access and type of authentication.

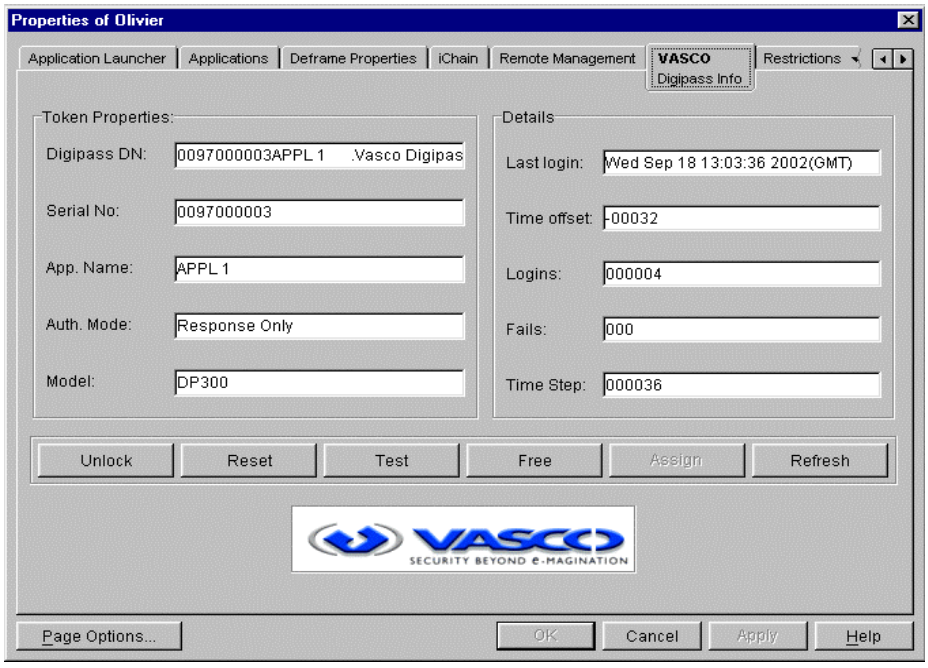


Fig 10.

By selecting the properties of a newly created user, a Digipass is assigned to that user. Fig.10 To be sure that the Digipass works fine, a test can be done by entering the values presented on the Digipass, into the required fields.

Activation Authentication Method –

VASCO Digipass Authentication

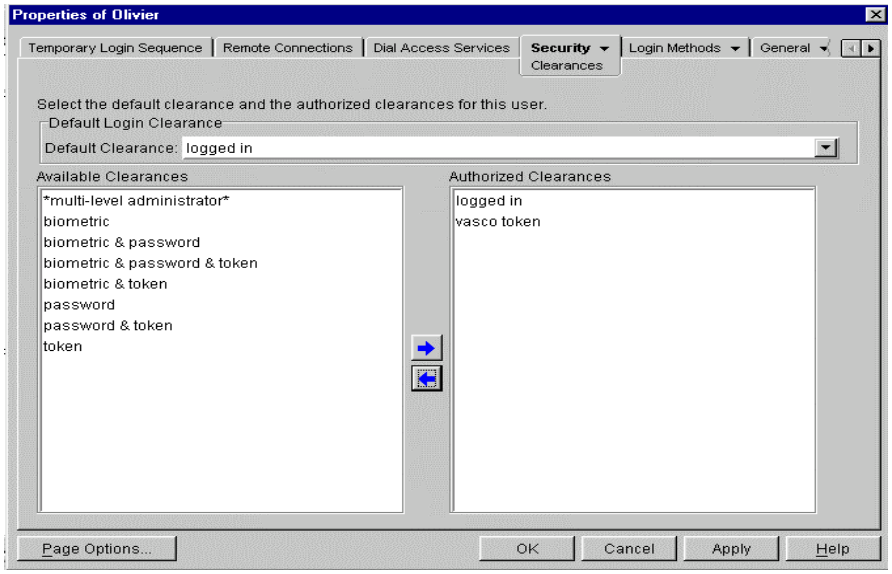


Fig 12

For each user select the authentication method. Here we select the VASCO token. Fig 12

Configuration of Radius

Novell

For detailed configuration of Radius within the Novell Radius Service, we refer you to visit http://www.novell.com

VASCO

As in this example we integrated Novell Radius Services. It's also possible to use VASCO Radius Services. For more information on these server products you can contact us at http://www.vasco.com

See appendix C

Novell

For more information regarding configuration or product details, we refer to
http://www.novell.com

Other web servers, services

In the current scenario we used the Novell web server. To find other web solutions VASCO has fully support on Apache or IIS.

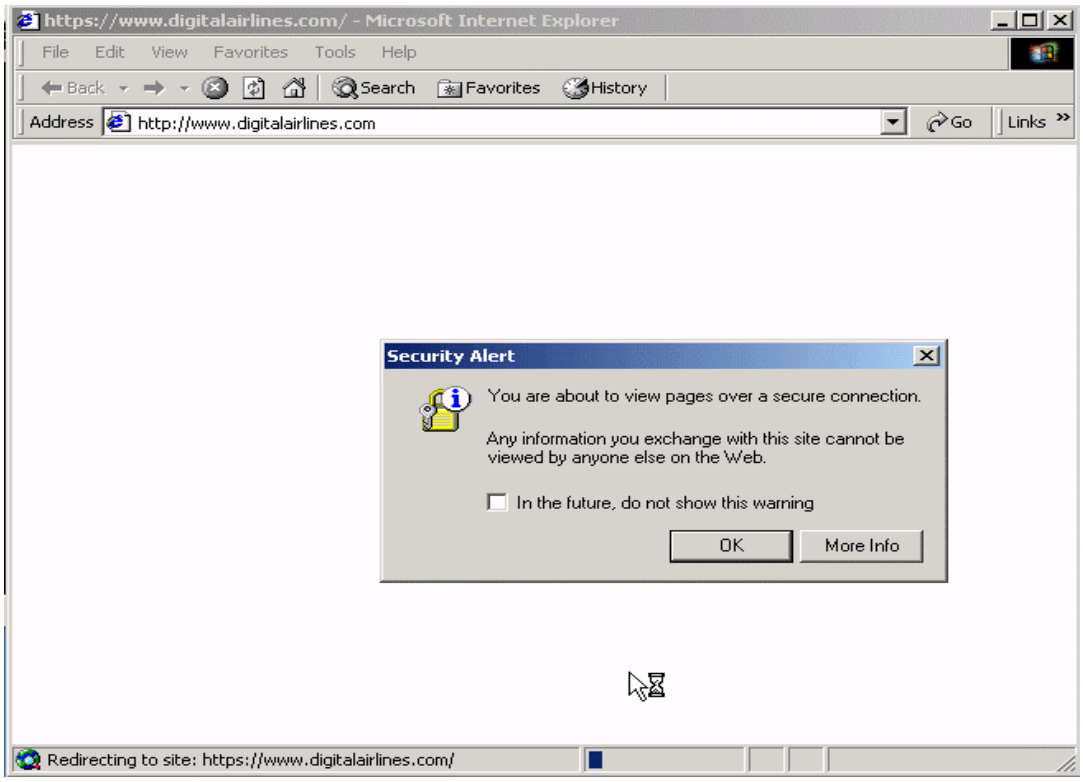
http://www.microsoft.com
http://www.apache.org

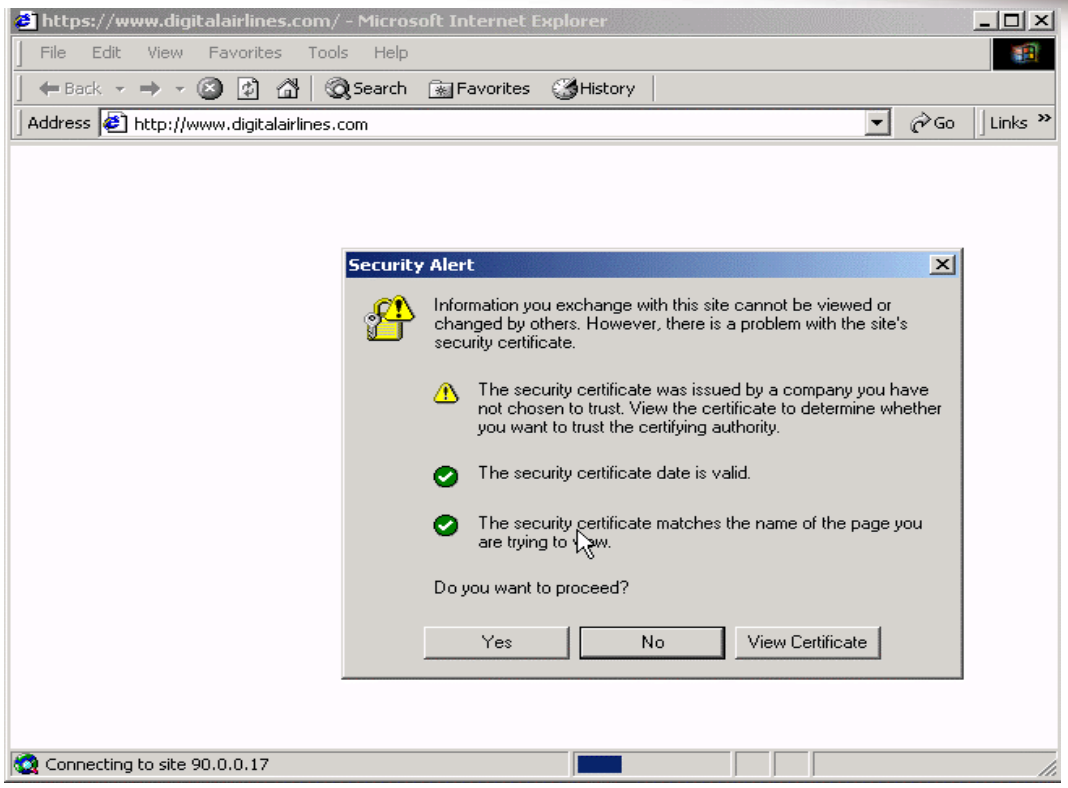
Conclusion

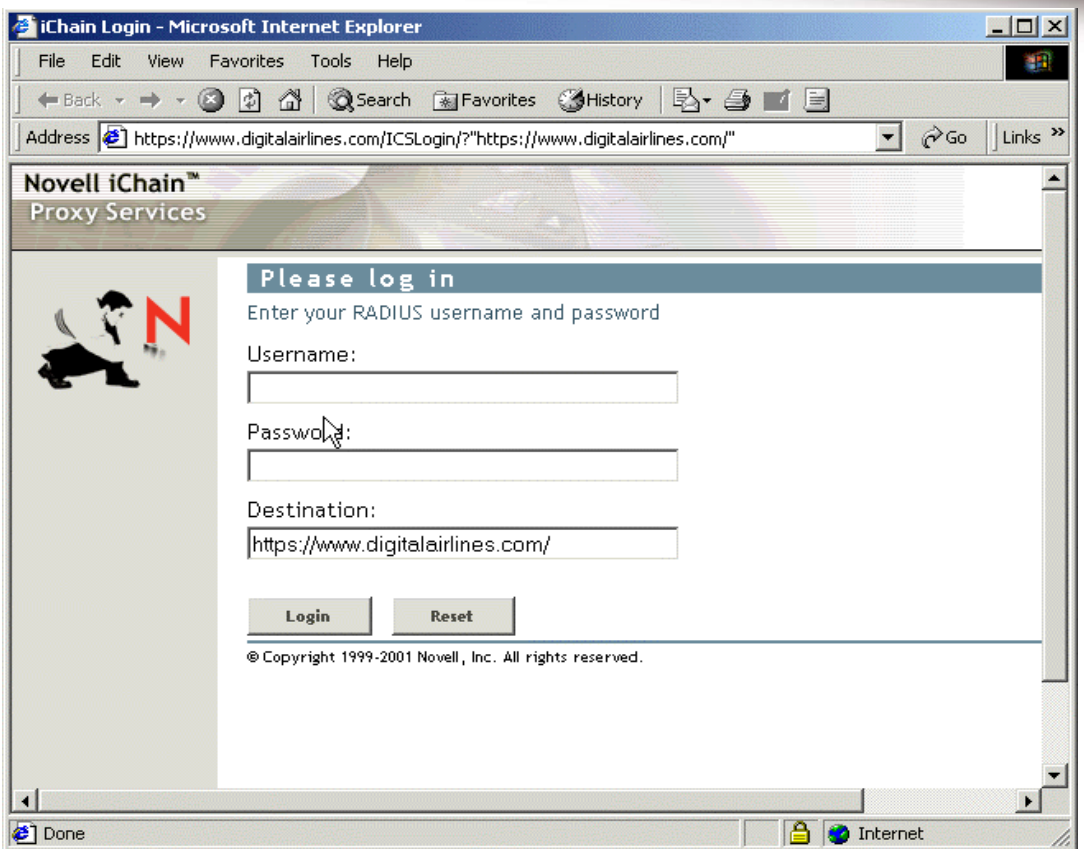
ICHAIN and NMAS with VASCO Digipass integration secures access from any location to applications and other resources inside your network with the luxury not having to deal with complex infrastructures. As the market has a variety in types of companies, the same way their applications or services will need to look and feel like. VASCO invented Digipasses and other systems to meet these demands. AnyWhere, AnyTime, AnyPlace.

Appendix A – Delta Airlines Access Examples

Authentication – Authorization over IChain secured


https://www.digitalairlines.com/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://www.digitalairlines.com
Go Links
Security Alert
You are about to view pages over a secure connection.
Any information you exchange with this site cannot be viewed by anyone else on the Web.
In the future, do not show this warning
OK
More Info
Redirecting to site: https://www.digitalairlines.com/

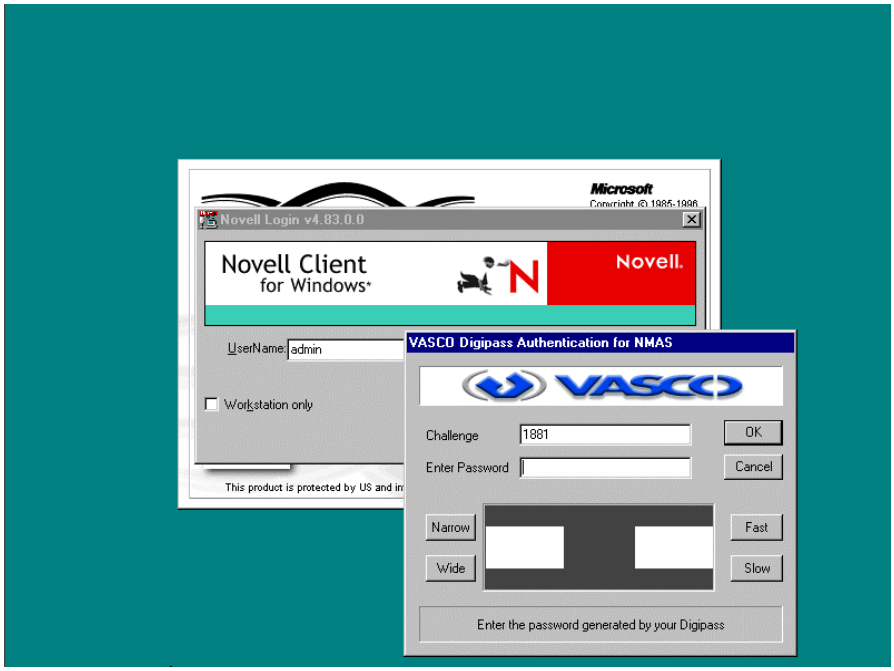

https://www.digitalairlines.com/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://www.digitalairlines.com
Go Links
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate matches the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate
Connecting to site 90.0.0.17


iChain Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://www.digitalairlines.com/ICSLogin/?"https://www.digitalairlines.com/"
Go Links
Novell iChain™
Proxy Services
Please log in
Enter your RADIUS username and password
Username:
Password:
Destination:
https://www.digitalairlines.com/
Login
Reset
© Copyright 1999-2001 Novell, Inc. All rights reserved.
Done
Internet

Appendix B Local Network Logon

VASCO – Challenge Response Authentication

Novell NMAS will present you the VASCO challenge which needs to be entered into a token in order to enter the correct response into the `Enter password` field.



Once authenticated by VASCO, NMAS presents the NDS static password as second verification. Authentication settings are configured on user basis (covered earlier in this paper).

Microsoft
Novell Login v4.83.0.0
Novell Client
for Window
Novell.
UserName: admin
Workstation only
NMAS NDS Password
Novell.
Modular Authentication Service
Password:
Change Password
OK
Cancel
This product is protected by

Appendix C – The VASCO VRM & Tokens work with BM (BMAS) VPN Services

VPN Secure Authentication with The Digipass 300 and the Digipass Go-1 with PIN+RESPONSE

When defining the Login Policy Rule for VPN, the External Login Service Method must be defined as MANDATORY. You cannot use "Required if assigned"

So, it is a global setting for anyone using VPN that will be required to use Token Authentication.

You will need to install the VRM from VASCO and get it working. (Test with a RADIUS client like NTRadPing).
Then, configure NDS as per TID 2952863: 3rd Party Authentication Server with BMEE3.5 (use method one).
When configuring the Login Policy Object Rule, Select VPN and add a Method. Browse to the External Login Service that was created using the TID. Make sure the make it MANDATORY.

About VASCO Data Security

General

VASCO Data Security International, Inc. (VDSI) designs, develops, markets and supports open standards-based software and hardware security products, which manage and secure access to information and financial assets. Securing trust, securing value is the company's creed. VASCO's range of enterprise-wide products secure Internet, client/server, and mainframe-based applications, and provide end-to-end security through RADIUS, LAN and Web security, PKI and LDAP enablement, web portal and application security, strong user authentication, access control, user administration and encryption.
VASCO's products are used by more than 7 million users, by over 180 financial institutions and by hundreds of blue-chip corporations and governments, spanning over 50 countries. VASCO is a global company with headquarters in the United States.

Company:	VASCO Data Security International
NASDAQ NM/NASDAQ EU.:	VDSI

Founded:	1997
Web:	www.VASCO.com
CEO	Ken Hunt
President and COO:	Jan Valcke
Employees:	80
Worldwide Headquarters:	1901 South Meyers Road, Suite 210, Oakbrook Terrace, Illinois, USA
European Headquarters:	Koningin Astridlaan 164, B-1780 Wemmel, Belgium
VASCO Product Range:	*VACMAN*: Authentication, Authorization, Administration, AAA Security *Digipass*: Encryption, Remote Access, Corporate Access, Hard- & software tokens

VASCO's roots are in cryptography. It was the first company in the world to port the DES and RSA algorithms to a chip and also the first to develop a software product to authenticate and digitally sign e-banking and online brokerage services. Now, VASCO secures the enterprise from the mainframe to the Internet with infrastructure solutions that enable secure e-business and e-commerce, while protecting sensitive information and safeguarding the identity of users. The company's family of Digipass® and VACMAN® products offer end-to-end security through strong authentication and digital signature, enterprise Single Sign-On, and LAN security, while sharply reducing the time and effort required to deploy and manage security.

Digipass product range

DIGIPASS® provides financial institutions and companies with a secure means of customer or employee identification and authentication for remote access to their computer systems and networks.

Digipass stands for three ranges:

Digipass Pro:

Digipass Pro includes Digipass models for professional use, offering dynamic password and digital signature functionality.

- Digipass Pro 300 is ideally suited for large public banking applications such as telebanking, home banking, PC banking, phone banking and Internet banking where authentication and e-signatures are key requirements.
- Digipass Pro 550 combines strong authentication, e-signatures and a modern design with integrated hardcover.
- Digipass Pro 600 grants physical access to buildings as well as secure remote network access.

- Digipass Pro 700 offers sophisticated and yet user-friendly strong authentication services with extended digital signature capability.
- Digipass Pro 800 is used by several top tier banking institutions
- worldwide and is strongly appreciated by the banks and their clients for securing full access to financial applications on the existing banking network via an existing smart card, in a flexible, easy to use and cost-effective way.

Digipass GO:

Digipass GO can be used Anywhere, Anyhow and Anytime. It is e-security that fits in your pocket, clips on your belt, hangs around your neck, on a key ring.

- Digipass GO 1 is the first-born in the "GO" range. GO 1 is an ultra-portable, smoothly designed token that outsmarts all others and is much safer than any static password.
- Digipass GO 10 is a software Digipass for GSM's, integrated on the SIM card.

Digipass Desk:

The Desk-range contains highly user friendly Digipass models to be used on a professional's desk.

- Digipass Desk 300 is a large-scale security device designed for managers and executives. It features remote access and authentication features and its larger size makes it very suitable for use in the office.
- Digipass Desk 850 can future-proof an existing smart card system, increase a network's security and leverage investment in a public key infrastructure (PKI) solution. This advanced e-wallet/PKI device provides ultimate versatility and security, supporting strong authentication and e-signatures for the customers authorized to carry your smart cards.
- Digipass Desk 3000 is a software Digipass for laptop & desktop.

VACMAN product range

VACMAN Controller integrates smoothly into existing applications that require remote access.

VACMAN RADIUS Middleware enables strong authentication security without replacing or redesigning your remote access solution(s).

VACMAN Server is a cross platform authentication engine designed to provide strong and seamless user authentication and access control for remote, local and web-based users. The product supports RADIUS, LAN and Web functionality.

- *VACMAN Server for RADIUS* is a standard compliant server designed to provide AAA services.

- *VACMAN Server for Networks* provides strong user authentication and access control management for RADIUS and LAN environments in a fully integrated system.
- *VACMAN Server for Web* delivers access control to Web enabled applications, whether Internet, extranet or intranet based.